

## REMARKS

In the Office Action mailed on June 4, 2004, claims 18 and 19 were rejected under 35 U.S.C. § 101; claim 10 was rejected under 35 U.S.C. § 112, second paragraph; and claims 1-15, 18 and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Srey et al (U.S. Patent No. 6,141,436) in view of Bongiorno et al. (U.S. Patent No. 6,292,045).

In accordance with the foregoing, claims 1, 10, 18 and 19 have been amended.

Claims 1-15, 18 and 19 are pending in the subject application.

Srey et al. discusses a portable communication device having a fingerprint identification system including a scanner for scanning a fingerprint and to generate an image of the fingerprint and to determine whether the scanned fingerprint matches an image of a reference fingerprint stored in a memory device of the portable communication device (see FIG. 6 and column 8, line 38 - column 9, line 20). The fingerprint identification system only recognizes unique personal fingerprints of a person to provide increased security against fraudulent use of the portable communication device (see column 3, lines 22-25). That is, if the scanned fingerprint matches a reference fingerprint, normal operation of the portable communication device is permitted (see column 9, lines 5-10).

Bongiorno et al. discusses a circuit for coupling between at least two clock sources and any device that requires clock pulses in order to operate. This circuit ensures that clock pulses from one of the clock sources are provided to such a device as long as one of the clock sources is operating (see column 2, lines 25-31). Bongiorno et al. further discusses a circuit for coupling between at least two clock sources and a timer of a microprocessor-based system or a microprocessor of such microprocessor-based system (see column 2, lines 31-34).

Neither Srey et al. nor Bongiorno et al., individually or combined, fail to discuss "a data converter comprising a data conversion unit to encrypt and decrypt data, a timer unit which counts time, and a lock system which locks a data conversion function of said data conversion unit in a disabled state and prevents data encryption and decryption, based on the time counted by said timer unit," as recited in amended claim 1 from which claims 2-15, directly or indirectly depend.

Nor do the foregoing references relied upon discuss all of the features recited in claim 18 from which claim 19 depends.

Each of claims 2-15 and 19 recites patentably distinguishing limitations of their own. For example, claim 12 recites "a time setting unit which sets a waiting time before the data conversion function is disabled".

The Applicants respectfully submit that the combination of Srey et al. and Bongiorno et al. fails to establish a prima facie case of obviousness. Therefore, claims 1-15, 18 and 19 patentably distinguish over Srey et al. in view of Bongiorno et al.

Withdrawal of the foregoing rejections is respectfully requested.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

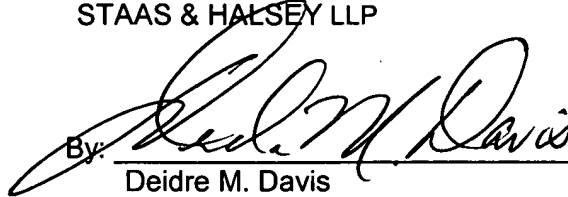
Respectfully submitted,

STAAS & HALSEY LLP

Date:

September 3, 2004

By:



Deidre M. Davis  
Registration No. 52,797

1201 New York Avenue, NW, Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501